BORDER BASIS REPRESENTATION OF A GENERAL QUOTIENT ALGEBRA

BERNARD MOURRAIN AND PHILIPPE TRÉBUCHET

Abstract. In this paper, we generalized the construction of border bases to non-zero dimensional ideals for normal forms compatible with the degree, tackling the remaining obstacle for a general application of border basis methods. First, we give conditions to have a border basis up to a given degree. Next, we describe a new stopping criteria to determine when the reduction with respect to the leading terms is a normal form. This test based on the persistence and regularity theorems of Gotzmann yields a new algorithm for computing a border basis of any ideal, which proceeds incrementally degree by degree until its regularity. We detail it, prove its correctness, present its implementation and report some experimentations which illustrate its practical good behavior.

1. Introduction

Solving polynomial equations is an ubiquitous problem which has a long mathematical history and many applications. An important approach to find all the (complex) solutions of a system of polynomial equations $f_1(x_1, \ldots, x_n) = 0, \ldots, f_s(x_1, \ldots, x_n) = 0$ is based on so-called "solving by quotient algebra" techniques. In this family of methods, the (complex) solutions of the system are recovered from the analysis of the quotient structure R/I where $R = \mathbb{K}[x_1, \ldots, x_n]$ is the ring of polynomials and $I = (f_1, \ldots, f_s)$ is the ideal generated by the polynomials $f_1, \ldots, f_s$.

This approach involves the construction of a projection with kernel I which maps R onto a vector space $\langle B \rangle$ spanned by a basis $B \subset R$ (usually of monomials) so that we have $R = \langle B \rangle \oplus I$. Such a projection, also called a normal form modulo the ideal I, can for instance be defined as a reduction with respect to a family of polynomials of I. F.S Macaulay [15] introduced the notion of an H-basis, which consists of generators of the ideal I with a normal form property for the reduction with respect to the components of highest degree. Replacing the usual graduation by a graduation associated to a monomial ordering, Gröbner bases (see [2] or [4] for a modern presentation) provide also a normal form property for the reduction with respect to the leading monomials for the given monomial ordering. By the simplicity of the reduction and the combinatorial information it can provide on R/I, it became a classical tool in computer algebra and effective commutative algebra. H-bases have not been as extensively used as there is no general algorithm for computing it : in [18] an algorithm is proposed but it relies on the a priori knowledge of a system of generator of the first syzygy module which cannot be expected to be known in advance in most situations and in [5] a numerical method is proposed provided some isolated points of the variety are known which also, cannot be expected to be easily found.

A less classical projection technique called border basis has been developed mostly over the last decade (see eg. [17, 19, 21, 11, 13, 12, 20, 3, 22, 10]). One

of the motivations was to handle numerical instability issues which structurally appear in Gröbner basis computation when dealing with approximate coefficients, as this is the case in many applications [20]. The main difference with previous graded reduction techniques is that the normal form property is related to the commutation property of operators of multiplication [19]. The approach offers more freedom to choose a basis B of the quotient algebra R/I adapted to the geometry of the solutions and provides a numerically stable normal form algorithm [22]. The border basis approach can be seen as a generalization of Gröbner basis computation in the case of zero-dimensional ideals. Indeed if the projection is compatible with a monomial ordering, a border basis is a Gröbner basis for this monomial ordering. Unfortunately, their study and construction were essentially restricted to zero-dimensional ideals. The goal of the paper is to describe a new method to compute border basis for any ideal.

Contributions. The border bases that we consider hereafter are related to a set B of monomials connected to 1 (see Section 2). They are more general than the one considered in [13, 11, 12, 3, 10], where B is assumed to be a set of monomials stable by division (called an order ideal).

We will not assume that B is known a priori or that the projection is compatible with a monomial ordering as in [13, 3], since this leads to the construction of Gröbner bases, with well-developed monomial rewriting techniques but also with numerical instability problems that we want to avoid.

For the sake of simplicity, we restrict the present article to projections compatible with the usual degree. This is not a conceptual limitation.

So far, border bases have been developed essentially for zero-dimensional ideals, except in [3] where the projection is compatible with a monomial ordering and thus leads to Gröbner basis computation.

The main contribution of this paper is to provide a new criterion of border bases for any projection compatible with the degree on a vector space spanned by a set B of monomials connected to 1. This criterion which applies to any ideal is based on the persistence and regularity theorems of G. Gotzmann [8].

The algorithm that we propose is an extension of the algorithm in [21] for zero-dimensional ideals. It exploits a new characterization of border bases up to a given degree, and proceeds incrementally degree by degree until the regularity criteria is satisfied. It is complete and has no possible case of "failure" as the algorithm for zero-dimensional ideals in [10]. As a byproduct, we obtain the Hilbert polynomial of the graded part of the ideal and thus the dimension and the degree of the solution set.

An implementation in C++ is also provided in the package `borderbasix` of the project MATHEMAGIX and we report on some experimentations which illustrate the practical good behavior of the method.

The paper is organized as follows. In the next section, we give the definitions we need. In Section 3, we prove the theoretical results involved in the algorithm, which is described in Section 4. In Section 5, we report on some benchmarks of an implementation before the concluding section.

2. NOTATIONS

Let $\mathcal{M}$ be the set of monomials in the variables $x_1, \ldots, x_n$. An element of $\mathcal{M}$ is of the form $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ with $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. Its degree is

$|\alpha| = \alpha_1 + \cdots + \alpha_n$. Let $R = \mathbb{K}[x_1, \ldots, x_n]$ be the ring of polynomials in the variables $x_1, \ldots, x_n$ with coefficients in a field $\mathbb{K}$. For $p = \sum_{\alpha \in A} p_\alpha \mathbf{x}^\alpha$ with $p_\alpha \neq 0$, A is the support of p and $\deg(p) = \max_{\alpha \in A} |\alpha|$.

For any set S, $\#S$ is its number of elements of S.

For $d \in \mathbb{N}$ and $F \subset R$, let $F_{\leq d}$ (resp. F_d) be the set of polynomials in F of degree $\leq d$ (resp. d).

For $f \in R$, let f^T be the homogeneous component of f of highest degree. Similarly for a set $F \subset R$, $F^T = \{f^T \mid f \in F\}$.

For $F \subset R$, let $\langle F \rangle$ be the $\mathbb{K}$-vector space spanned by F. Let $F^+ = F \cup x_1 F \cup \cdots x_n F$ and $\partial F = F^+ \setminus F$. For $d \in \mathbb{N}_+$, let $F^{\langle \leq d \rangle} = \{m\, f \mid m \in \mathcal{M}, f \in F, \deg(m\, f) \leq d\}$ and $F^{\langle d \rangle} = F^{\langle \leq d \rangle} \setminus F^{\langle \leq d-1 \rangle}$.

A set $B \subset \mathcal{M}$ is *connected to* 1 if $1 \in B$ and $\forall m \in B \setminus \{1\}$, there exists $1 \leq i \leq n$ and $m' \in B$, such that $m = x_i\, m'$.

For a sequence F of polynomials in R and a sequence B of monomials in $\mathcal{M}$, $(F|B)$ is the matrix of coefficients of the polynomials in F for the monomials of B; a row of this matrix represents the coefficients of a polynomial in F; the order for the rows (resp. columns) is the order of the elements in the sequence F (resp. B).

3. Theoretical Results

Let $B \subset \mathcal{M}$ be a set of monomials connected to 1 and let $d \in \mathbb{N}$.

In this section, we assume that we are given a *projection* $\pi : \langle B^+ \rangle_{\leq d} \to \langle B \rangle_{\leq d}$ such that $\pi \circ \pi = \pi$ and $\pi_{|\langle B \rangle_{\leq d}}$ is the identity map, which is compatible with the degree: $\forall b \in \langle B^+ \rangle_{\leq d}$, $\deg(\pi(b)) \leq \deg(b)$. The kernel $\ker \pi$ of this projection is spanned by the elements:

$$f_\alpha = \mathbf{x}^\alpha - \pi(\mathbf{x}^\alpha), \mathbf{x}^\alpha \in (\partial B)_{\leq d}.$$

We denote by F this generating set of polynomials of $\ker \pi$ and call it the *rewriting family* of π.

Our objective is to characterize the projections π which are the restriction of a projection $\tilde{\pi} : R \to \langle B \rangle$ such that $I := \ker \tilde{\pi}$ is the ideal generated by $\ker \pi$. In such a case, we have $R = \langle B \rangle \oplus I$ and $\tilde{\pi}$ is a normal form modulo the ideal I.

The main idea behind border basis techniques is to relate this normal form property to commutation properties of multiplication operators [19]. We define the operator of multiplication by x_i associated to π as:

$$\begin{array}{rcl} M_i : \langle B \rangle_{\leq d-1} & \to & \langle B \rangle_{\leq d} \\ b & \mapsto & \pi(x_i b). \end{array}$$

As π is compatible with the degree, the image by M_i of an element of degree $\leq k$ is of degree $\leq k+1$ for $0 \leq k < d$.

For a monomial $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} \in \mathcal{M}$ of degree $\leq d$, we define $\mathbf{x}^\alpha(\mathbf{M}) := M_1^{\alpha_1} \circ \cdots \circ M_n^{\alpha_n}$. It is an operator from $\langle B \rangle_{\leq d-|\alpha|}$ to $\langle B \rangle_{\leq d}$. We extend this construction by linearity and for any $p \in R_{\leq d}$, we define

$$p(\mathbf{M}) : \langle B \rangle_{\leq d - \deg(p)} \to \langle B \rangle_{\leq d}.$$

As we will see, the commutation property of the multiplication operators M_i is related to the projection of the following polynomials.

Definition 3.1. *For $F \subset R$ and $B \subset \mathcal{M}$, let $\mathcal{C}_B(F)$ be the set of polynomials in $\langle B^+ \rangle$ which are of the form*

1) $x_i f$ *with* $f \in F$ *or*
2) $x_i f - x_j f'$ *with* $f, f' \in F$, $1 \leq i < j \leq n$.

The polynomials in $\mathcal{C}_B(F)$ *are called the commutation polynomials of* F *for* B.

The subset of $\mathcal{C}_B(F)$ satisfying condition 1 (resp. 2) is denote by $\mathcal{C}_B^1(F)$ (resp. $\mathcal{C}_B^2(F)$), so that $\mathcal{C}_B(F) = \mathcal{C}_B^1(F) \cup \mathcal{C}_B^2(F)$. In the following, the set B will be fixed and we will simply write $\mathcal{C}_B(F) = \mathcal{C}(F)$. From this definition, we have $\mathcal{C}(F) \subset \langle F^+ \rangle \cap \langle B^+ \rangle$.

Next, we describe different equivalent conditions for a normal form in degree $\leq d$. This theorem summarizes results which can be deduced from results in [19], [21], [22].

Theorem 3.2. *Let* $d \geq 2$, *let* B *be a subset of* $\mathcal{M}$ *connected to* 1, *let* $\pi : \langle B^+ \rangle_{\leq d} \to \langle B \rangle_{\leq d}$ *be a projection and let* F *be the rewriting family of* π. *The following conditions are equivalent:*

(1) $(M_i \circ M_j - M_j \circ M_i)_{|\langle B \rangle_{\leq d-2}} = 0$ *for* $1 \leq i < j \leq n$,
(2) *there exists a unique projection* $\tilde{\pi} : R_{\leq d} \to \langle B \rangle_{\leq d}$ *such that the restriction of* $\tilde{\pi}$ *to* $\langle B^+ \rangle_{\leq d}$ *is* π *and* $\ker \tilde{\pi} = \langle F^{\langle \leq d \rangle} \rangle$,
(3) $\langle (F_{\leq d-1})^+ \rangle \cap \langle B^+ \rangle \subset \langle F \rangle$,
(4) $\forall r \in \mathcal{C}(F_{\leq d-1})$, $\pi(r) = 0$.

Proof. 1) $\Rightarrow$ 2) : As B is connected to 1, $1 \in B$ and we can define

$$\begin{array}{rcl} \tilde{\pi} : R_{\leq d} & \to & \langle B \rangle_{\leq d} \\ p & \mapsto & p(\mathbf{M})(1) \end{array}$$

This construction is independent of the order in which we compose the operators M_i since they are commuting.

Let us show that $\tilde{\pi}$ is a projection of $R_{\leq d}$ on $\langle B \rangle_{\leq d}$, which extends π and such that $\ker \tilde{\pi} = \langle F^{\langle \leq d \rangle} \rangle$.

We first prove by induction on the degree that $\forall m \in B$, $\tilde{\pi}(m) = m$. The monomial of degree 0 of B is 1 and by definition $\tilde{\pi}(1) = 1$. The property is true for degree 0. Assume that it is true for degree $0 \leq k - 1 < d$ and let $m \in B$ be a monomial of degree k. As B is connected to 1, there exists $1 \leq i \leq n$ and $m' \in B$ of degree $k - 1$ such that $m = x_i\, m'$. As the operators M_i are commuting and as $\pi_{|\langle B \rangle_{\leq d}} = \mathrm{Id}$, we have by induction hypothesis

$$\tilde{\pi}(m) = M_i(m'(\mathbf{M})(1)) = \pi(x_i\, m') = m.$$

In particular, for any $b \in \langle B \rangle$ we have $b(\mathbf{M})(1) = b$.

We now prove that $\forall m \in (\partial B)_{\leq d}$, $\tilde{\pi}(m) = \pi(m)$. As $m \in \partial B$, there exist $m \in B$ and $0 \leq i \leq n$ such that $m = x_i\, m$. Thus we have

$$\tilde{\pi}(m) = M_i(m'(\mathbf{M})(1)) = \pi(x_i\, m') = \pi(m).$$

In the next step, we prove that $\langle F^{\langle \leq d \rangle} \rangle \subset \ker \tilde{\pi}$. For $m \in \mathcal{M}$ and $\mathbf{x}^\alpha \in \partial B$ with $\deg(m) + |\alpha| \leq d$, we show that $m\,(\mathbf{x}^\alpha - \pi(\mathbf{x}^\alpha)) \in \ker \tilde{\pi}$: As $\tilde{\pi}$ coincides with π on

$\langle B^+\rangle_{\leq d}$ and $\pi(\mathbf{x}^\alpha) \in \langle B\rangle$, we have

$$\begin{aligned}
&\tilde{\pi}(m\,(\mathbf{x}^\alpha - \pi(\mathbf{x}^\alpha)))\\
&= m(\mathbf{M}) \circ \mathbf{M}^\alpha(1) - m(\mathbf{M})(\pi(\mathbf{x}^\alpha)(\mathbf{M})(1))\\
&= m(\mathbf{M}) \circ \mathbf{M}^\alpha(1) - m(\mathbf{M})(\pi(\mathbf{x}^\alpha))\\
&= m(\mathbf{M}) \circ \mathbf{M}^\alpha(1) - m(\mathbf{M})(\tilde{\pi}(\mathbf{x}^\alpha))\\
&= m(\mathbf{M}) \circ \mathbf{M}^\alpha(1) - m(\mathbf{M})(\mathbf{M}^\alpha(1)) = 0
\end{aligned}$$

Finally, we prove that $R_{\leq d} = \langle B\rangle_{\leq d} \oplus \langle F^{\langle \leq d\rangle}\rangle$. For any $m \in \mathcal{M}$ of degree $1 \leq k \leq d$, there exist $m' \in \mathcal{M}$ of degree $k-1$ and $1 \leq i \leq n$ such that $m = x_i m'$. We have

$$m - \tilde{\pi}(m) = x_i(m' - \tilde{\pi}(m')) + (x_i\tilde{\pi}(m') - \tilde{\pi}(x_i m')).$$

By induction on the degree, we have $(m' - \tilde{\pi}(m')) \in \langle F^{\langle \leq k-1\rangle}\rangle$ and $x_i\tilde{\pi}(m') - \tilde{\pi}(x_i m') = x_i\tilde{\pi}(m') - \pi(x_i\tilde{\pi}(m')) \in F$. This shows that $m - \tilde{\pi}(m) \in \langle F^{\langle \leq k\rangle}\rangle$. As for any $p \in R_{\leq d}$, $p = \tilde{\pi}(p) + p - \tilde{\pi}(p)$, we deduce that $R_{\leq d} = \langle B\rangle_{\leq d} + \langle F^{\langle \leq d\rangle}\rangle$. As $\langle F^{\langle \leq d\rangle}\rangle \subset \ker\tilde{\pi}$ and $\tilde{\pi}_{|\langle B\rangle_{\leq d}} = \mathrm{Id}$, we have

$$R_{\leq d} = \langle B\rangle_{\leq d} \oplus \langle F^{\langle \leq d\rangle}\rangle,$$

with $\langle F^{\langle \leq d\rangle}\rangle = \ker\tilde{\pi}$.

2) $\Rightarrow$ 3) : Let $f \in \langle (F_{\leq d-1})^+\rangle \cap \langle B^+\rangle$. Then as $\langle (F_{\leq d-1})^+\rangle \subset \langle F^{\langle \leq d\rangle}\rangle = \ker\tilde{\pi}$, we have $\tilde{\pi}(f) = 0$. But $\tilde{\pi}$ coincides with π on $\langle B^+\rangle$ so that we have $\pi(f) = 0$, which shows that $f \in \ker\pi = \langle F\rangle$.

3) $\Rightarrow$ 4) : Clearly, if $r \in \mathcal{C}(F_{\leq d-1})$ then $r \in \langle (F_{\leq d-1})^+\rangle \cap \langle B^+\rangle$. By hypothesis (3), $r \in \langle F\rangle = \ker\pi$ and $\pi(r) = 0$.

4) $\Rightarrow$ 1) : Let $m \in B$ of degree $\leq d-2$ and $1 \leq i < j \leq n$. Suppose that $m_1 := x_i m \in \partial B$ and $m_2 := x_j m \in \partial B$. Let $f_1 = m_1 - \pi(m_1), f_2 = m_2 - \pi(m_2) \in F$. As $x_i m_2 = x_j m_1 = x_i x_j m$, we have

$$\begin{aligned}
&(M_i \circ M_j - M_j \circ M_i)(m)\\
&= \pi(x_i\pi(m_2)) - \pi(x_j\pi(m_1))\\
&= \pi(x_i(m_2 - f_2) - x_j(m_1 - f_1))\\
&= \pi(x_j f_1 - x_i f_2).
\end{aligned}$$

As $x_j f_1 - x_i f_2 = x_i\pi(m_2) - x_j\pi(m_1) \in \mathcal{C}(F_{\leq d})$, the hypothesis (4) implies that $\pi(x_j f_1 - x_i f_2) = 0$. A similar argument applies if $x_i m \in B$ or $x_j m \in B$. Consequently, we have $(M_i \circ M_j - M_j \circ M_i)_{|\langle B\rangle_{\leq d-2}} = 0$. □

If one of these (equivalent) conditions is satisfied, we say that the rewriting family F is a *border basis* in degree $\leq d$ for B.

Remark 3.3. *As a border basis in degree $\leq d$ contains a border basis in degree $\leq k$ for $0 \leq k \leq d$, this theorem implies that the restriction of $\tilde{\pi}$ to $R_{\leq k}$ is the projection onto $\langle B\rangle_{\leq k}$ along $\langle F^{\langle \leq k\rangle}\rangle$.*

Remark 3.4. *We can define a projection $\tilde{\pi} : R_{\leq d} \to \langle B\rangle_{\leq d}$ such that for any $\mathbf{x}^\alpha \in \mathcal{M}_{\leq d}$, $\tilde{\pi}(\mathbf{x}^\alpha) = \mathbf{M}^\alpha(1) \in \langle B\rangle_{\leq d}$ and we extend it by linearity on $R_{\leq d}$. Any order in the composition of the operators M_i can be used to define a projection $\tilde{\pi}$ on a specific monomial of degree $\leq d$. For any of these choices, we have a projection such that $\forall p \in R_{\leq d}, p - \tilde{\pi}(p) \in \langle F^{\langle \leq d\rangle}\rangle$ (see 3).*

However, if the operators M_i commute in degree $\leq d-2$, then this projection $\tilde{\pi}$ is uniquely defined.

We are now going to show that a border basis in degree $\leq d$ is an H-basis when d is big enough. The notion of H-basis introduced by F.S. Macaulay [15] corresponds to a generating set of an ideal, which allows to compute normal forms by reduction with respect to the components of highest degree. We recall that F is an H-basis of an ideal I if $F \subset I$ and $(F^T) = I^T$. A characterization of an H-basis involves syzygies that we define now:

Definition 3.5. *For $F = \{f_1, \ldots, f_l\} \subset R$ and $k \in \mathbb{N}$,*

$$\mathrm{Syz}_{\leq k}(F) \quad = \{ \quad \mathbf{r} = (r_1, \ldots, r_l) \in R^l \mid \textstyle\sum_{i=1}^{l} r_i f_i = 0 \text{ and } \\ deg(r_i f_i) \leq k \text{ for } 1 \leq i \leq l \quad \}$$

denotes the vector space of syzygies of F in degree $\leq k$.

We denote by $\mathrm{Syz}(F) = \cup_k \mathrm{Syz}_{\leq k}(F)$ the R-module of syzygies of F. We define by induction the i-th module of syzygies of F as the syzygy module of a minimal set of generators of the $(i-1)$-th module of syzygies, the 1-st syzygy module of F being $\mathrm{Syz}(F)$ (see eg. [6]).

For $H = \{h_1, \ldots, h_l\} \subset R$ and $\mathbf{r} \in \mathrm{Syz}(F)$, let $\mathbf{r}(H) = \sum_{i=1}^{l} r_i h_i \in R$.

Here is a characterization of H-basis in terms of syzygies (see [15], [18] or [7][Theorem 2.14, p.33]):

Theorem 3.6. *Let $F \subset R$, $G = F^T$, $I = (F)$ and $\{\mathbf{r}_1, \ldots, \mathbf{r}_s\}$ a generating family of $\mathrm{Syz}(G)$. F is an H-basis of I iff for all $1 \leq i \leq s$,*

$$\mathbf{r}_i(F) \in \langle F^{\langle \leq l_i \rangle} \rangle \text{ where } l_i = \deg(\mathbf{r}_i(F)).$$

We prove now that for a border basis F in degree $\leq d$, the syzygies of F^T lift to syzygies of F:

Proposition 3.7. *Assume that F is a border basis in degree $\leq d$. Then for any $\mathbf{r} \in \mathrm{Syz}_{\leq k}(G)$, $0 \leq k \leq d$, we have $\mathbf{r}(F) \in \langle F^{\langle \leq l \rangle} \rangle$ where $l = \deg(\mathbf{r}(F)) < k$.*

Proof. If F is a border basis in degree $\leq d$, by Theorem 3.2(2), $\tilde{\pi}(\mathbf{r}(F)) = 0$ since $\mathbf{r}(F) \in \langle F^{\langle \leq k \rangle} \rangle$. As $\mathbf{r}(G) = 0$, $\mathbf{r}(F)$ is of degree $l < k$. By remark 3.3, as $\tilde{\pi}$ is the projection from $R_{\leq l}$ onto $\langle B \rangle_{\leq l}$ along $\langle F^{\langle \leq l \rangle} \rangle$, we deduce that $\mathbf{r}(F) \in \langle F^{\langle \leq l \rangle} \rangle$. □

This proposition allows us to show that a border basis in degree $\leq d$ is an H-basis when d is bigger than the regularity of (F^T).

We recall that the (Castelnuovo-Mumford) regularity of an homogeneous ideal $J \subset R$, denoted $\mathrm{reg}(J)$, is the minimum m such that J is generated in degree $\leq m$, and the k-th module of syzygies of J is generated in degree $\leq m+k$ for $k = 1, \ldots, n$ (see [6][chap. 4, p. 55]). We say that J is d-regular if $\mathrm{reg}(J) \leq d$.

Theorem 3.8. *Let B be a subset of $\mathcal{M}$ connected to 1, F a border basis in degree $\leq d$ for B, and $G = F^T$. If $J = (G)$ is $(d-1)$-regular then F is an H-basis of $I = (F)$.*

Proof. By definition of the regularity, $\mathrm{Syz}(G)$ has a generating set of syzygies $\mathbf{r}_1, \ldots, \mathbf{r}_s \in \mathrm{Syz}_{\leq d}(G)$ of degree less than d. By Proposition 3.7, we have $\mathbf{r}_i(F) \in \langle F^{\langle \leq l_i \rangle} \rangle$ where $l_i = \deg(\mathbf{r}_i(F)) < d$ and we deduce by Theorem 3.6 that F is an H-basis for $I = (F)$. □

Corollary 3.9. *Let B be a subset of $\mathcal{M}$ connected to 1, F a border basis in degree $\leq d$ for B and $G = F^T$. Then B_k is a basis of $R_k/(G)_k$ for $0 \leq k \leq d$.*

Proof. By Remark 3.3, for any polynomial $p \in R_{\leq k}$ of degree $k \leq d$, we have $p = f + b$ with $f \in \langle F^{\langle \leq k \rangle} \rangle$, $b \in \langle B \rangle_{\leq k}$. Taking the components of degree k of each term in this decomposition, we have $p^T = f_k + b_k$ with $f_k \in \langle G^{\langle k \rangle} \rangle$, $b_k \in \langle B_k \rangle$. This shows that $R_k = \langle G^{\langle k \rangle} \rangle + \langle B_k \rangle$. Let $p = \langle G^{\langle k \rangle} \rangle \cap \langle B_k \rangle$. As $p \in \langle G^{\langle k \rangle} \rangle$ there exists $f \in \langle F^{\langle \leq k \rangle} \rangle$ such that $p' = p - f \in R_{\leq k-1}$ so that $\tilde{\pi}(p) = \tilde{\pi}(p') = p$ with $p \in R_k$ and $p' \in R_{\leq k-1}$. As $\tilde{\pi}$ is compatible with the degree, this implies that $p = p' = 0$ and we have

$$R_k = \langle G^{\langle k \rangle} \rangle \oplus \langle B_k \rangle.$$

As G is an homogeneous family of polynomials $\langle G^{\langle k \rangle} \rangle = (G)_k$ and B_k is a monomial basis of $R_k/(G)_k$. □

Our next objective is to characterize the regularity of a homogeneous ideal J in terms of the dimension $H_{R/J}(d) = \dim R_d/J_d$ ($H_{R/J}$ is called the Hilbert function of R/J). The first problem we consider is how to determine when the sequence fo integers $\alpha = \{\alpha_0, \alpha_1, \alpha_2, \dots\}$ is the Hilbert function of R/J for some homogeneous ideal J. This problem was solved by F.S. Macaulay, using the following decomposition: for any integer $\nu \in \mathbb{N}$ and $i \in \mathbb{N}_+$, there exists a unique sequence of integers $g_i > \cdots > g_1 \geq 0$ such that

$$\nu = \binom{g_i}{i} + \cdots + \binom{g_1}{1},$$

assuming that $\binom{g}{h} = 0$ if $g < h$. This decomposition is denoted by $\nu^{\langle i,0 \rangle}$. For $k \in \mathbb{N}$, we write $\nu^{\langle i,k \rangle} = \binom{g_i+k}{i+k} + \cdots + \binom{g_1+k}{1+k}$.

A theorem of Macaulay [16] says that the integer sequence $\nu = \{\nu_0, \nu_1, \nu_2, \dots\}$ is the Hilbert function of a homogeneous ideal $\neq R$ if and only if $\nu_0 = 1$ and $\nu_{i+1} \geq {\nu_i}^{\langle i,1 \rangle}$ for all $i \geq 1$. This theorem is based on the analysis of ideals L_J generated in degree i by the $H_R(i) - H_{R/J}(i)$ first monomials for the lexicographic ordering for all $i \in \mathbb{N}$. The monomial ideal L_J is called the lex-segment ideal of J.

Two other interesting results on Hilbert functions are proved in [9][Theorems 3.8 and 3.11], [1][Theorems 4.3.2 and 4.3.3] (see also [8]):

Theorem 3.10. *Let J be a homogeneous ideal in the polynomial ring $R = \mathbb{K}[x_1, \dots, x_n]$. Set $\nu_i = dim_k(R/J)_i$ for $i \geq 0$. Let s be such that $\nu_{s+1} = {\nu_s}^{\langle s,1 \rangle}$ and assume that J is generated in degrees $\leq s+1$ then*

1. *(Gotzmann's Persistence Theorem) ${\nu_i}^{\langle i,1 \rangle} = {\nu_s}^{\langle s,i+1-s \rangle}$ for all $i \geq s$.*
2. *(Gotzmann's Regularity Theorem) $\mathrm{reg}(J) \leq s$.*

The property that the lex-segment L_J has a Hilbert function with minimal growth is used to prove these results.

Remark 3.11. *The condition $\nu_{s+1} = {\nu_s}^{\langle s,1 \rangle}$ is reached for some degree $s \in \mathbb{N}$, since it means that the lex-segment ideal L_J associated to J is generated in degrees $\leq s$.*

Theorem 3.12. *Let B be a subset of $\mathcal{M}$ connected to 1, F a border basis in degree $\leq d$ for B, $\nu_{d-1} = \#B_{d-1}$, $\nu_d = \#B_d$. If $\nu_d = {\nu_{d-1}}^{\langle d-1,1 \rangle}$, then F is an H-basis of $I = (F)$.*

Proof. Let $G = F^T \subset R_{\leq d}$ and $J = (G)$. By Corollary 3.9, $H_{R/J}(d-1) = \nu_{d-1}$, $H_{R/J}(d) = \nu_d$. By Theorem 3.10(2) $\mathrm{reg}(J) \leq d-1$. By Theorem 3.8, F is an H-basis of $I = (F)$. □

This theorem allows us to recover the Hilbert function of $J = (F^T)$ and thus numerical invariants such as the dimension of the solutions of $F = 0$ or the degree. For $\nu \in \mathbb{N}$ with a d-th decomposition $\nu^{\langle d,0\rangle} = \binom{g_d}{d} + \cdots + \binom{g_1}{1}$ with $g_d > \cdots > g_1 \geq 0$, we define $\lambda_d(\nu) = \max_{0\leq i\leq d}(g_i - i)$ and $\delta_d(\nu) = \#\{i \mid g_i - i = \lambda_d(\nu), 0 \leq i \leq d\}$.

Corollary 3.13. *Let B be a subset of $\mathcal{M}$ connected to 1, F a border basis in degree $\leq d$ for B, $\nu_k = \#B_k$ for $0 \leq k \leq d$ with $\nu_d = {\nu_{d-1}}^{\langle d-1,1\rangle}$, $I = (F)$, $J = I^T$. Then*

- *$H_{R/J}(i) = {\nu_{d-1}}^{\langle d-1,i-d+1\rangle}$ for $i \geq d-1$,*
- *R/I is of (algebraic) dimension $\lambda_{d-1}(\nu_{d-1}) + 1$,*
- *The degree of R/I is $\delta_{d-1}(\nu_{d-1})$ if $\lambda_{d-1}(\nu_{d-1}) \geq 0$ and $\sum_k \nu_k$ otherwise.*

Proof. By Theorem 3.10(1), the Hilbert function of R/J (or R/L_J) is given for $i \geq d-1$ by

$$\begin{aligned} H_{R/J}(i) &= {\nu_{d-1}}^{\langle d-1,i-(d-1)\rangle} \\ &= \binom{g_{d-1}+i-d+1}{i} + \cdots + \binom{g_1+i-d+1}{i-d+2} \\ &= \binom{i+g_{d-1}-(d-1)}{g_{d-1}-(d-1)} + \cdots + \binom{i+g_1-(d-1)}{g_1-1} \end{aligned}$$

where $\nu_{d-1} = \binom{g_{d-1}}{d-1} + \cdots + \binom{g_1}{1}$ with $g_{d-1} > \cdots > g_1 \geq 0$. Let $\lambda := \lambda_{d-1}(\nu_{d-1})$ and $\delta := \delta_{d-1}(\nu_{d-1})$. If $\lambda \geq 0$, $H_{R/J}(i)$ expands as a polynomial in i which highest degree term is $\frac{\delta}{\lambda!} i^\lambda$. Thus the dimension of R/J (resp. R/I) is λ (resp. $\lambda+1$) and its degree is δ. If $\lambda \leq 0$, then B_{d-1} is empty, B is finite and its number of elements $\sum_k \nu_k$ is the degree of R/I. □

Remark 3.14. *If $\nu_d = {\nu_{d-1}}^{\langle d-1,1\rangle}$, we also have that* $\operatorname{reg}(J) \leq d-1$ *so that $J = I^T$ and I are generated in degree $\leq d-1$, and the k-th module of syzygies of J and I are generated in degree $d+k-1$ for $0 \leq k \leq n$.*

*In this case, generators of a H-*basis *and of its first syzygy module of are known in degree d and we will stop the border computation and say the $F = \ker \pi$ is an H-border basis.*

4. Algorithm

The algorithm presented in this section allows us to compute a border basis representation of the quotient by any ideal up to a degree where the generators form an H-basis (see Remark 3.14). It consists of constructing incrementally degree by degree a monomial set B connected to 1 together with a projection π from $\langle B^+\rangle$ onto B and to test if the commutation condition of Theorem 3.2(1) is satisfied up to a given degree. If the commutation property is not satisfied, new polynomials are deduced and used to update the set B and the projection π. This computation is repeated until the regularity test is satisfied.

To compute such a set B, we will use the same strategy as the one described in [21], which relies on a *choice function*.

Definition 4.1. *A* choice function *γ is a function from R to $\mathcal{M}$, such that given a polynomial f, $\gamma(f)$ is one of the monomials of the support of f. We say that a* choice function refines the degree *if the returned monomial is of maximal degree among the monomials of f.*

This choice function can be the function which "chooses" the leading monomial for a given monomial ordering. In this case we shall obtain a Gröbner basis. But it can be more general and not necessarily related to a monomial ordering of $\mathcal{M}$ which is compatible with the multiplication by monomials. It can also take into account the numerical value of the coefficients (see examples in [21]).

This choice function will be used to select monomials outside B. In the following, the set B will be a union of intersections of monomial ideals with the complement of other monomial ideals.

The computation is made more efficient by an early *prediction* of what should be B and by checking that the prediction is correct up to a given degree. This is done by projecting a small set of polynomials, namely the commutation polynomials, in order to check the condition (4) of Theorem 3.2. When the projected polynomials are not 0, they are used to update the projection so that they belong to the kernel of the new projection. This computation is repeated until the regularity test of Theorem 3.10 is satisfied for a set B and a degree d.

We now state the algorithm of computation of H-border bases, which is based on the algorithm described in [21]:

Algorithm 4.1: H-border basis

Input: A set of polynomials $\mathcal{F} = \{f_1, \ldots, f_s\}$ and γ a choice function refining the degree.

Output: A H-border basis for $I = (f_1, \ldots, f_s)$.

- $Initialization(k, F_k, B, \mathcal{F})$
- While $not(is\_reg?(B, k))$ or $k < \max_{f\in\mathcal{F}} \deg(f)$;
  - (1) Compute $C^1_{k+1} := \mathcal{C}^1_B(F_k)$ and $A_{k+1} := (B^+)_{k+1}$.
  - (2) Construct the matrix $M_{k+1} := (C^1_{k+1}|A_{k+1})$.
  - (3) Compute $r_{k+1} := \operatorname{rank} M_{k+1}$.
  - (4) If $\langle C^1_{k+1}\rangle$ contains polynomials of degree $< k+1$, add them to $\mathcal{F}$ and start a new loop with $k := \min_{p\in C^1_{k+1}} \deg(p)$.
  - (5) If $\#(A_{k+1} \setminus B_{k+1}) \neq r_{k+1}$,
    - compute $A'_{k+1} \subset A_{k+1}$ such that $\#A'_{k+1} = r_{k+1} = \operatorname{rank}(F_{k+1} \mid A'_{k+1})$; for instance looking at the monomials indexing the columns of a maximal invertible submatrix of M_{k+1}.
    - compute $B'_{k+1} = A_{k+1} \setminus A'_{k+1}$;
    - add the monomials B'_{k+1} to B;
  - (6) Define $\pi_{k+1} : \langle B^+\rangle_{\leq k+1} \to \langle B\rangle_{\leq k+1}$ as the extension of π_k such that $C^1_{k+1} \subset \ker \pi_{k+1}$ and F_{k+1} as the new polynomials of degree $k+1$ in the corresponding rewriting family.
  - (7) Compute $C^2_{k+1} := \pi_{k+1}(\mathcal{C}^2_B(F_k)) \cup \tilde{\pi}_{k+1}(\mathcal{F}_{k+1})$.
  - (8) If $C^2_{k+1} = \{0\}$, then start new loop with $k := k+1$.
  - (9) If $\langle C^2_{k+1}\rangle$ contains polynomials of degree $< k+1$, add them to $\mathcal{F}$ and start a new loop with $k := \min_{p\in C^2_{k+1}} \deg(p)$.
  - (10) Apply γ to $\langle C^2_{k+1}\rangle$, remove the monomial ideal generated by $\gamma(\langle C^2_{k+1}\rangle)$ from B and update $\pi_{k+1} : \langle B^+\rangle_{\leq k+1} \to \langle B\rangle_{\leq k+1}$ and F_{k+1}, so that $C^2_{k+1} \subset \ker \pi_{k+1}$.

The function $Initialization(k, F_k, B, \mathcal{F})$ performs initializing steps:

- Find a linearly independent set of polynomials, F_k, of minimum degree, k, from $\mathcal{F}$. (a basis of the $\mathbb{K}$-*vector subspace* spanned by the polynomials of minimum degree of the $\mathbb{K}$-vector generated by $\mathcal{F}$).
- Define B as the monomial set $\mathcal{M}\backslash(\gamma(F_k))$.

The regularity test $is\_reg?(B, d)$ is implemented as follows:

Algorithm 4.2: Regularity test

Input: A set of monomials B and a degree d.
Output: A boolean indicating that the ideal has reached Gotzmann persistence.

- Compute $\nu = dim_{\mathbb{K}}(\langle B\rangle_{d-1})$.
- Compute the Macaulay decomposition $\nu^{\langle d-1,0\rangle}$ of ν.
- If $dim_{\mathbb{K}}(\langle B\rangle_d) = \nu^{\langle d,1\rangle}$ then return true; else return false;

For steps 4 and 5, a triangulation of M_{k+1} is computed. The choice function γ is used to select the pivots. The rank of M_{k+1} is read off from the triangular form. The transformation on the rows of M_{k+1} are reported on the polynomial vector C^1_{k+1}. The zero-rows of the triangulation yield the polynomials of degree $< k+1$ in $\langle C^1_{k+1}\rangle$.

In step 5, the monomials B'_{k+1} are added to B by updating the representation of B as a union of intersections of monomial ideals with the complementary of other monomial ideals. Only the monomials of B'_{k+1} are added to this description but not their multiples. By construction, this yields a new set B of monomials, which is connected to 1.

In step 6, to define the projection π_{k+1} from $(B^+)_{\leq k+1}$ to $\langle B\rangle_{\leq k+1}$, we invert $(F_{k+1} \mid A'_{k+1})$, and construct new elements in $\langle F_{k+1}\rangle$ with one monomial in A'_{k+1} and the other monomials in B. This defines the new set F_{k+1} of polynomials of degree $k+1$ of the rewriting family associated to π_{k+1}.

In step 7, the commutation polynomials $\mathcal{C}^2_B(F_k) \subset \langle B^+\rangle_{\leq k+1}$ are projected on $\langle B\rangle_{\leq k+1}$ by π and the elements $\mathcal{F}_{k+1}$ of degree $k+1$ of $\mathcal{F}$ are projected on $\langle B\rangle_{\leq k+1}$ by $\tilde{\pi}$ (see Remark 3.4).

For steps 9 and 10, a triangulation of the coefficient matrix $(C^2_{k+1} \mid B_{k+1})$ is also computed by applying the choice function γ to select the pivots. This transformation is then used to update B and F_{k+1}.

For more details on these computations, see [21].

Notice that in the update of B (step 5), it can happen that the set B is extended and not reduced (some monomials are added to B). These are cases where algorithms as in [10] fail to construct a basis B stable by division (see eg. [10, Step (T7), Prop. 3.8]), showing that it is necessary to consider more general families of monomial bases B which are connected to 1, if we want to deal with general choice functions.

The previous algorithm is correct and stops after a finite number of steps on any input as we prove now.

We recall here Lemma 4.6 of [21] which proof also applies our case:

Lemme 4.2. *For all $d \in \mathbb{N}$, there exist finitely many F_k containing polynomials whose leading monomials are of degree less than d.*

This lemma is used to prove the termination of the H-border basis algorithm:

Theorem 4.3. *The algorithm stops for some k and outputs a H-border basis of $I = (f_1, \ldots, f_s)$.*

Proof. The monomial set B maintained in the algorithm is connected to 1 by construction.

By Lemma 4.2, for every degree k_0 there exists an iteration of the `While` loop, from which k does not drop under $k_0 + 1$. Hence for each $k \in \mathbb{N}$, the set F_k if defined becomes unchanged at a certain point in the algorithm.

As R is noetherian, the sequence of ideals $(\cup_{i \leq k} F_i^T)$ eventually becomes stationary. Let J be this ideal.

Again, according to Lemma 4.2, Theorem 3.10, Corollary 3.9 and Remark 3.11, there exists an iteration of the `While` loop such that all commutation polynomials project to 0 by π_k, J is generated in degree $\leq k-1$ and the regularity test applies. Theorem 3.8 allows us to conclude the proof. □

5. Implementation/Benchmarks

We have implemented the previous algorithm in C++. It is available in the package `borderbasix` of the project Mathemagix[1]. We report here on its experimentation. The main criterion, Macaulay decomposition and Gotzman persistence test correspond to approximately 200 lines. Less than 3000 lines (among 200000) had to be modified in the implementation of [21] in order to handle efficiently the regularity criterion (this includes the computation of the list of monomials in B at degree k).

We report first a comparision between the zero dimensional implementation of [21] and the one with the regularity test. As the polynomials computed are the same with or without the criterion, and in order to emphasize the overhead introduced here we perform computation with the smallest type of coefficients available in the package `borderbasix`, i.e. modular coefficients with support in 16-bit integers.

We use here a choice function that chooses one monomial of maximal partial degree among the available monomials (named `mac` in [21]).

The experiments reported here have been performed on a Core2 Duo 2.26GHz, with 4Go of DDR2 800Mhz with a 64bit linux 3.2 kernel.

Example	*nv*	*deg*	*time*	*memory*	*Isreg*
*kat*8	8	256	0.5*s*	40*M*	0.001*s*
*kat*9	9	512	3.49*s*	55*M*	0.002*s*
*kat*10	10	1024	26.66*s*	79*M*	0.002*s*
*cyclic*5	5	70	0.16*s*	20*M*	0.001*s*

In this table, *nv* is the number of variables, *deg* the degree of the quotient algebra R/I, *time* the average time (over 1000 runs) for the whole computation in seconds, *memory* the memory size used by the test, $Isreg$ the time spent in the regularity test in seconds.

As it can be seen, the overhead introduced by the new regularity test is completely negligible compared to the rest of the computation.

[1] `www.mathemagix.org`

We report here the timings and degree stop for some examples; the notation `-neq` means that n equations have been discarded.

Example	*nv*	*time*	*memory*	*Isreg*	*choice*
$kat5-1eq$	5	$0.66s$	$15M$	16	*grevlex*
$kat5-1eq$	5	$0.36s$	$5M$	16	*mac*
$kat5-2eq$	5	$2.36s$	$5M$	24	*mac*
$kat6-1eq$	6	$1.06s$	$5M$	32	*mac*
$kat7-1eq$	7	$455s$	$35M$	64	*mac*
$cyclic5-1eq$	5	$0.25s$	$5M$	24	*grevlex*
$cyclic6-1eq$	6	$84.96s$	$36M$	156	*grevlex*
butcher	7	–	$500M$	38	*mac*

There is a huge difference in time between kastura n and the same problem with one equation discarded. This comes from the difference of size of the matrices to be inverted and from the fact that one has to go much further in degree. The difference of behavior with respect to the choice function is somehow masked here, the coefficient growth does not appear as the degree increases.

It is interesting to notice that Gotzman persistence is detected in degree more than the Castelnuovo Mumford regularity. It is the subject of a further work to improve the stopping criterion.

6. Conclusion

We have presented an extension of the border basis algorithm of [21], which computes a border basis description of the quotient by any ideal up to any degree. This algorithm stops at a degree bigger than or equal to the regularity of the ideal. It outputs an H-basis of the ideal and its Hilbert polynomial. The stopping criterion exploits a characterization of a border basis up to a given degree, in terms of the projection of commutation polynomials and the persistence and regularity theorems of Gotzmann. A C++ implementation is also provided and some benchmarks illustrate the good practical behavior of the approach.

Though this new method addresses the main drawback of border basis methods, namely the restriction to zero-dimensional ideals, all is not said on this topic. Several interesting problems remain open. One of them is to relate the stopping degree more closely with the regularity of the ideal. Further investigations are also needed to analyze the syzygy modules of the border basis along the lines developed in [22]. The approach has also potential applications in relaxation methods used to compute radicals or real radicals [14], when the (real) radical is not zero dimensional. Generalizing the method to projections not necessarily compatible with the degree should also be detailled and implemented.

References

[1] W. Bruns and J. Herzog. *Cohen-Macaulay rings*, volume 39 of *Cambridge Studies in Advanced Mathematics*. Academic Press, 1983.

[2] B. Buchberger. *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German)*. PhD thesis, Math. Inst, Univ. of Innsbruck, Austria, 1965. (also in Aequationes Math. 4/3, 1970).

[3] Yufu Chen and Xiaohui Meng. Border bases of positive dimensional polynomial ideals. In *Proceedings of the 2007 international workshop on Symbolic-numeric computation*, SNC '07, pages 65–71, New York, NY, USA, 2007. ACM.

[4] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition, 1997.
[5] Barry H. Dayton. Numerical calculation of h-bases for positive dimensional varieties. In *Proc. SNC 2011*, pages 8–16, San Jose, California USA, 2011.
[6] D. Eisenbud. *The geometry of syzygies*, volume 229 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.
[7] M. Elkadi and B. Mourrain. *Introduction à la résolution des systèmes polynomiaux*, volume 59 of *Mathématiques et Applications*. Springer, 2007.
[8] G. Gotzmann. Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes. *Math. Z.*, 158:61–70, 1978.
[9] M. Green. Generic initial ideals. In *Six lectures on commutative algebra*, volume 166 of *Progress in Mathematics*, pages 119–185. Birkhauser, 1998.
[10] Stefan Kaspar. Computing border bases without using a term ordering. *Beiträge zur Algebra und Geometrie / Contributions to Algebra and Geometry*, pages 1–13, 2011.
[11] A. Kehrein and M. Kreuzer. Characterizations of border bases. *J. Pure Appl. Algebra*, 196(2-3):251–270, 2005.
[12] A. Kehrein and M. Kreuzer. Computing border bases. *J. Pure Appl. Algebra*, 205(2):279–295, 2006.
[13] M. Kreuzer and L. Robbiano. *Computational Commutative Algebra 2*. Springer, Heidelberg, 2005.
[14] J.B. Lasserre, M. Laurent, and P. Rostalski. Semidefinite Characterization and Computation of Zero-Dimensional Real Radical Ideals. *Foundations of Computational Mathematics*, 8(5):607–647, 2008.
[15] F.S. Macaulay. *The Algebraic Theory of Modular Systems*. Cambridge Univ. Press, 1916.
[16] F.S. Macaulay. Some Properties of Enumeration in the Theory of Modular Systems. *Proc. London Math. Soc.*, 26:531–555, 1927.
[17] M. G. Marinari, H. M. Möller, and T. Mora. Gröbner bases of ideals given by dual bases. In *Proceedings of the 1991 international symposium on Symbolic and algebraic computation*, ISSAC '91, pages 55–63, New York, NY, USA, 1991. ACM.
[18] H. M. Möller and T. Sauer. H-bases for polynomial interpolation and system solving. *Adv. Comput. Math.*, 12(4):335–362, 2000.
[19] B. Mourrain. A new criterion for normal form algorithms. In M. Fossorier, H. Imai, Shu Lin, and A. Poli, editors, *Proc. AAECC*, volume 1719 of *LNCS*, pages 430–443. Springer, Berlin, 1999.
[20] B. Mourrain. *Symbolic-Numeric Computation*, chapter Pythagore's Dilemma, Symbolic-Numeric Computation, and the Border Basis Method, pages 223–243. Trends in Mathematics. Birkhäuser, 2007.
[21] B. Mourrain and Ph. Trébuchet. Generalised normal forms and polynomial system solving. In M. Kauers, editor, *International Conference on Symbolic and Algebraic Computation*, pages 253–260, Beijing, China, 2005. ACM New York, NY, USA.
[22] B. Mourrain and Ph. Trébuchet. Stable normal forms for polynomial system solving. *Theoretical Computer Science*, 409(2):229–240, 2008.

Bernard Mourrain, GALAAD INRIA Méditerranée, BP 93, 06902 Sophia Antipolis, France

E-mail address: Bernard.Mourrain@inria.fr

Philippe Trébuchet, Equipe APR. LIP6, UPMC/CNRS, 4 place Jussieu, 75256 Paris Cedex

E-mail address: Philippe.Trebuchet@lip6.fr